IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants:	Boon HO et al.	§	Confirmation No.:	8413
Serial No.:	10/717,521	§	Group Art Unit:	2474
Filed:	11/21/2003	§	Examiner:	Feben Haile
For:	Method And System For Monitoring A Network Containing Routers Using A Backup Routing Protocol	§	Docket No.:	200310819-1

APPEAL BRIEF

Mail Stop Appeal Brief – Patents
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Date: June 25, 2010

Sir:

Appellants hereby submit this Appeal Brief in connection with the above-identified application. A Notice of Appeal was electronically filed on May 14, 2010.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest is Hewlett-Packard Development Company, L.P. (HPDC), a Texas Limited Partnership, having its principal place of business in Houston, Texas. HPDC is a wholly owned affiliate of Hewlett-Packard Company (HPC). The Assignment from the inventors to HPDC was recorded on April 20, 2004, at Reel/Frame 015234/0996.

II. RELATED APPEALS AND INTERFERENCES

Appellants are unaware of any related appeals or interferences.

III. STATUS OF THE CLAIMS

Originally filed claims:	1-37.
Claim cancellations:	None.
Added claims:	None.
Presently pending claims:	1-37.
Presently appealed claims:	1-37.

IV. STATUS OF THE AMENDMENTS

No claims were amended after the Office Action dated March 26, 2010.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

This section provides a concise explanation of the subject matter defined in each of the independent claims, referring to the specification by page and line number or to the drawings by reference characters as required by 37 C.F.R. § 41.37(c)(1)(v). Each element of the claims is identified with a corresponding reference to the specification or drawings where applicable. The specification references are made to the application as filed by Appellants. Note that the citation to passages in the specification or drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element. Also note that these specific references are not exclusive; there may be additional support for the subject matter elsewhere in the specification and drawings.

Some embodiments are directed to a method as in claim 1:

1. A method for monitoring a network containing routers using a backup routing protocol and organized in at least one backup router group,[1] comprising:

discovering a topology object model of the routers;[2]

detecting a condition of the at least one backup router group based on at least one threshold value;[3] and

displaying an indication of the detected condition.[4]

[1] Fig. 1; p. 8, ¶ [0025], lines 1-2; p. 10, ¶ [0033], lines 1-3.

[2] Fig. 1 102; p. 8, ¶ [0025], line 3; p. 10, ¶ [0033], lines 4-5.

[3] Fig. 1 104; p. 8, ¶ [0025], line 5; p. 10, ¶ [0033], lines 10-11.

[4] Fig. 2 106; p. 8, ¶ [0025], line 5; p. 10, ¶ [0033], lines 10-11.

Other embodiments are directed to a system as in claim 12:

12. A system for monitoring a network containing routers using a backup routing protocol and organized in at least one backup router group,[5] comprising:

means for discovering a topology object model of the routers and detecting a condition of the at least one backup router group based on at least one threshold value;[6] and

means for displaying an indication of the detected condition.[7]

Yet other embodiments are directed to a computer readable medium as in claim 24:

24. A computer readable medium comprising a computer program embedded therein for causing a computer to perform:[8]

discovering a topology object model of routers included within a network;[9]

detecting a condition of at least one backup router group of the routers based on at least one threshold value;[10] and

displaying an indication of the detected condition.[11]

---

[5] Fig. 3; p. 8, ¶ [0026], lines 1-2; p. 18, ¶ [0053], lines 1-2.

[6] Fig. 3 330; p. 8, ¶ [0026], lines 3-5; p. 18, ¶ [0053], lines 3-4.

[7] Fig. 3 310; p. 8, ¶ [0026], line 5; p. 18, ¶ [0053], lines 6-7.

[8] Fig. 3; p. 8, ¶ [0025], lines 5-7; p. 25, ¶ [0067], lines 12-14.

[9] Fig. 3 330; p. 8, ¶ [0025], line 3; p. 25, ¶ [0067], line 3.

[10] Fig. 3 330; p. 8, ¶ [0025], lines 3-4; p. 25, ¶ [0067], line 4.

[11] Fig. 3 310; p. 8, ¶ [0025], line 5; p. 25, ¶ [0067], lines 9-10.

Further embodiments are directed to a data structure embodied within a computer readable medium as in claim 35:

35. A data structure embodied within a computer readable medium for representing a backup routing protocol topology object model for a network, the data structure[12] comprising:

at least one network node object representing an element in the network;[13]

at least one network interface object for each at least one network node object, the at least one network interface object representing an interface of the network element corresponding to the each at least one network node object;[14]

an address object for each at least one network interface object, representing an address of the corresponding interface;[15]

a backup routing protocol group object representing network elements organized in a backup routing protocol group, the backup routing protocol group object including a virtual address of the backup routing protocol group and real addresses of the network elements in the backup routing protocol group;[16] and

an address state object for each of the real addresses of the network elements in the backup routing protocol group, including a state of the corresponding address.[17]

---

[12] Fig. 2 200; p. 8, ¶ [0027], lines 1-2; p. 15, ¶ [0049], lines 1-3.

[13] Fig. 2 204; p. 8, ¶ [0027], lines 3-4; p. 15, ¶ [0049], line 4.

[14] Fig. 2 206; p. 8-9, ¶ [0027], lines 4-5; p. 15, ¶ [0049], lines 4-6.

[15] Fig. 2 212; p. 9, ¶ [0027], lines 6-7; p. 15, ¶ [0049], lines 8-9.

[16] Fig. 2 202; p. 9, ¶ [0027], lines 8-11; p. 15, ¶ [0049], lines 10-12.

[17] Fig. 2 216; p. 9, ¶ [0027], lines 11-13; p. 15, ¶ [0049], lines 19-20.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1, 3-6, 9-12, 14-17, 20-24, 26-29 and 32-37 are obvious under 35 U.S.C § 103(a) over Ofek et al. (U.S. Pub. No. 2004/0083284, hereinafter "*Ofek*") in view of Liu et al. (U.S. Pat. No. 7,197,660, hereinafter "*Liu*").

Whether claims 2, 7-8, 13, 18, 19, 25, 30, and 31 are obvious under 35 U.S.C § 103(a) over *Ofek* in view of *Liu* and further in view of Yip et al. (U.S. Pat. No. 6,954,436, hereinafter "*Yip*").

VII. ARGUMENT

A. Rejections Under 35 U.S.C. § 103(a) Over *Ofek* and *Liu*

1. Independent Claim 1

Appellants respectfully traverse the rejection of independent claim 1, as *Ofek* and *Liu* fail to teach or suggest Appellants' invention as set forth in claim 1. Consequently, the Examiner has failed to establish a prima facie case of obviousness in combining *Ofek* and *Liu* to reject independent claim 1.

Independent claim 1 method recites, among other features, discovering a topology object model of routers, and detecting a condition of at least one backup router group based on at least one threshold value. Claim 1 also recites displaying an indication of the detected condition. Such features are neither taught nor suggested by the documents relied upon by the Examiner, such that claim 1 is allowable.

More particularly, in rejecting claim 1 the Examiner referred to paragraph [0021] of *Ofek*,[18] and admitted that *Ofek* "fails to explicitly suggest detecting a condition of the at least one backup router group based on at least one threshold value."[19] However, the Examiner asserted that it would have been obvious to "incorporate the recovery method taught by *Liu* into the system for providing data awareness disclosed by *Ofek*."[20] This assertion of the Examiner is respectfully traversed. Appellants respectfully disagree with the Examiner's ultimate conclusion. Even assuming, arguendo, that a motivation to combine is somehow interjected as suggested by the Examiner, the presently claimed invention would not have resulted.

Referring to Appellants' exemplary Figure 1 embodiment, a method is disclosed for monitoring a network that includes routers that use a backup routing protocol. Exemplary embodiments use a topology object model, such as the data structure shown in Appellants' Figure 2, to monitor the network. No such

---

[18] *Office Action*, p. 3 (Mar. 26, 2010).

[19] *Id.*

[20] *Id.*

topology object model is disclosed or suggested in any of the references relied upon by the Examiner, nor is any method or system which exploits such a topology object model disclosed or suggested.

Ofek is directed to using a topology object model[21] to store elements of different types of domains (*e.g.*, the SONET-based domain and the DWDM-based domain).[22] There is no discussion in *Ofek* of configuring a network to contain routers that use a backup routing protocol, and that are organized in at least one backup router group. As such, there is no teaching or suggestion in *Ofek* of any mechanism for discovering topology information concerning such routers, or for evaluating conditions of such routers. *Ofek* therefore fails to provide teaching or suggestion of detecting a condition of at least one backup router group based on a threshold value, as recited in Appellants' claim 1. Because there are no routers which use a backup routing protocol that are discovered in *Ofek*, and no detecting of any condition associated with a backup router group containing such routers, *Ofek* also fails to disclose or suggest the claim 1 feature of displaying any indication of such a detected condition.

Liu is directed to a network security system wherein a master device and backup device within a cluster of network security devices, are provided. *Liu* describes detecting failure in the cluster of network security devices, and using the state information to recover from the failure.[23] *Liu* shows in Fig. 2 a recovery system 202 which has a memory 208 and a controller 206. Memory 208 contains a redundancy group table 210, a master data partition 212 and a backup data partition 214. Each security device 102 is assigned to one or more redundancy groups and each redundancy group is assigned to host a certain set of connections. Within each redundancy group, one security device is designated the master, another security device is designated the primary backup, and the remaining security devices in the redundancy group are designated as secondary

---

[21] *Ofek*, ¶ [0021].

[22] *Ofek*, ¶¶ [0005], [0008].

[23] *Liu*, Abstract.

backups.[24] However, this disclosure of a "security device" in *Liu* does not relate specifically to routers that use a backup routing protocol, and therefore does not disclose at least one backup router group. As such, there is no teaching or suggestion in *Liu* of any mechanism for discovering topology information concerning such routers, or for evaluating conditions of such routers.

Liu further discloses a path monitor 228 which detects failures of other devices within the cluster 110 (*i.e.*, not local failures). The Examiner appears to have taken out of context the mention of a path monitor 228 containing a failure threshold parameter that defines the threshold for what constitutes a "failure" for other devices or paths in the system.[25] However, at least for the reasons as set forth above, this "threshold" disclosure of *Liu* that the Examiner relies on is not specifically related to detecting a condition of at least one backup router group based on a threshold value, as presently recited in Appellants' claim 1.

Liu mentions a redundancy group so that a "next master" can be pre-selected before a failure occurs in the network affecting the originally identified master device.[26] However, this again relates to "security devices." There is no teaching or suggestion in *Ofek* or in *Liu* of detecting a condition of a backup router group based on a threshold value, and displaying an indication of such a detected condition as part of a network monitoring operation as required by independent claim 1. *Ofek* and *Liu* do not relate to backup router groups. Further, *Liu* does not deal with display of backup router group information. Further, neither *Ofek* nor *Liu* deals with detecting and displaying conditions of a backup router group.

Therefore, *Ofek* and *Liu* fail to teach or suggest the limitations of independent claim 1. Appellants respectfully request that the rejections of claims 1, 3-6, and 9-11 be reversed and the claims set for issue.

---

[24] *Liu*, col. 4, lines 21-30.

[25] *Liu*, col. 5, lines 17-25.

[26] *Liu*, col. 8, lines 10-29.

2. Independent Claims 12 and 24

Independent claims 12 and 24 include limitations similar to those of claim 1 explained above. For example, claim 12 recites a system for monitoring a network wherein a discovering means discovers a topology object model of routers using a backup routing protocol, and detecting a condition of at least one backup router group based on a threshold value; and displaying an indication of the detected condition. Independent claim 24 is directed to a computer readable medium including similar features. Therefore, Appellants respectfully submit that the Examiner erred in rejecting independent claims 12 and 24, and claims 14-17, 20-23, 26-29, and 32-34 for much the same reasons as are given above with regard to independent claim 1. Appellants respectfully request that the rejections be reversed and the claims set for issue.

3. Independent Claim 35

Independent claim 35 is directed to a data structure embodied within a computer readable medium for representing a backup routing protocol topology object model for a network. The data structure requires, "a backup routing protocol group object representing network elements organized in a backup routing protocol group." Such a feature enables an exemplary embodiment wherein conditions of a backup routing group can be detected and displayed. The Examiner admitted that *Ofek* fails to teach these limitations,[27] and cited *Liu* Fig. 1 110 and col. 4, lines 21-30 as allegedly so teaching. The cited portions of *LIU* teach a cluster of device (*i.e.*, a redundancy group) but fail to teach or suggest a backup routing protocol group object of a data structure as required by claim 35.

Claim 35 also requires that "the backup routing protocol group object include[es] a virtual address of the backup routing protocol group and real addresses of the network elements in the backup routing protocol group." The Examiner admitted that *Ofek* fails to teach these limitations,[28] and cited *Liu*

[27] *Office Action*, p. 10 (Mar. 26, 2010).

[28] *Office Action*, p. 10 (Mar. 26, 2010).

col. 10, lines 36-34 as allegedly so teaching.[29] The cited portion of *Liu* teaches that each device has its own IP and MAC address. However, *Liu* fails to teach or suggest that either of these addresses is a virtual address or a virtual address of the backup routing protocol group.

For at least these reasons, in conjunction with the reasons given with regard to similar limitations of claim 1, Appellants respectfully submit that the Examiner erred in rejecting independent claim 35, and claims 36-37 depending therefrom. Appellants respectfully request that the rejections be reversed and the claims set for issue.

4. Claims 3, 14, and 26

Claims 3, 14, and 25 require that "the detecting is also based on a number of backup router groups to which one of the routers belongs." The Examiner cited *Liu* col. 8, lines 49-51 as allegedly teaching these limitations. The cited portion of *Liu* teaches that each device acts as a master in one redundancy group and a backup in other groups. However, *Liu* fails to teach or suggest that detecting a condition of a backup router group is based on a number of groups to which a router belongs. That a device belongs to multiple groups is inapposite to the required detecting being based on a number of groups to which a router belongs. *Ofek* fails to satisfy this deficiency of *Liu*. For at least these additional reasons, Appellants respectfully submit that the Examiner erred in rejecting claims 3, 14, and 26.

5. Claims 5, 16, and 28

Claims 5, 16, and 28 require that the topology object model comprise "a state of at least one of the at least one address that is external to the backup router group." The Examiner cited *Liu* col. 5, lines 11-16 as allegedly teaching these limitations. The cited portion of *Liu* teaches that the "self-monitor 224 detects local failures." Thus, any state related to detected failures is internal rather than external. Furthermore, *Liu* fails to teach or suggest that state is of an address external to the group or that the state is stored in the topology object

[29] Appellants assume the Examiner intended lines 36-38.

model. *Ofek* fails to satisfy these deficiencies of *Liu*. For at least these additional reasons, Appellants respectfully submit that the Examiner erred in rejecting claims 5-6, 16-17, and 28-29.

6. Claims 6, 17, and 29

Claims 6, 17, and 29 require that the "detecting is also based on the state of the at least one address that is external to the backup router group." The Examiner cited *Liu* col. 5, lines 11-16 as allegedly teaching these limitations. The cited portion of *Liu* teaches that the "self-monitor 224 detects local failures." Thus, the failures detected are local rather than "external to the backup router group." *Ofek* fails to satisfy this deficiency of *Liu*. For at least these additional reasons, Appellants respectfully submit that the Examiner erred in rejecting claims 6, 17, and 29.

7. Claim 36

Claim 36 requires that the data structure include "a track interface object corresponding to a tracked network interface of a first network element in the backup routing protocol group wherein the tracked network interface is located between the first network element and a network element outside the backup routing protocol group." The Examiner cited *Liu*, col. 5, lines 11-16 as allegedly teaching these limitations. The cited portion of *Liu* teaches a "self-monitor 224 that detects local failures." However, the existence of the self-monitor 224 fails to teach or suggest a track interface object in a data structure representing a backup routing protocol topology object, but rather merely teaches existence of a local failure detection mechanism. Moreover, the self-monitor of *Ofek* fails to teach or suggest that the tracked network interface is located between the first network element and a network element outside the backup routing protocol group. *Ofek* fails to satisfy this deficiency of *Liu*. For at least these additional reasons, Appellants respectfully submit that the Examiner erred in rejecting claim 36.

8. Claim 37

Claim 37 requires that for the data structure "each network interface object is related to one or more address objects." The Examiner cited *Ofek*, Fig. 4 105 as allegedly teaching these limitations. *Ofek*, Fig. 4 depicts an object that

describes characteristics of a SAN switch.[30] Consequently, the device IP address 105 is the SAN switch IP address. Thus, *Ofek* teaches an object for a device, such as a SAN switch, that includes the IP address 105 of the device. A device object is different from a network interface object as indicated by the limitations of claim 37 requiring that "each network node object is related to one or more network interface objects." Consequently, *Ofek* fails to teach or suggest that "each network interface object is related to one or more address objects." *Liu* fails to satisfy this deficiency of *Ofek*.

Similarly, claim 37 requires that for the data structure "address object is related to one or more network interface objects." The Examiner cited *Ofek*, Fig. 4 109 and 110 as allegedly teaching these limitations. However, recording the number of ports 109 and the world wide name 110 of a device in a device object fail to relate an address object to an interface object at least because neither the port count 109 nor WWN 110 are interface objects. *Liu* fails to satisfy this deficiency of *Ofek*.

For at least these additional reasons, Appellants respectfully submit that the Examiner erred in rejecting claim 37.

B. Rejections Under 35 U.S.C. § 103(a) Over *Ofek*, *Liu*, and *Yip*

Claims 2, 7, and 8 depend from independent claim 1. Claims 13 and 18 depend from independent claim 12. Claims 25 and 30 depend from independent claim 24. *Yip* fails to satisfy the deficiencies of *Ofek* and *Liu* explained above with regard to claims 1, 12, and 24. Therefore, Appellants respectfully submit that the Examiner erred in rejecting claims 2, 7, 8, 13, 18, 19, 25, 30, and 31 for much the same reasons as are given above with regard to independent claims 1, 12, and 24.

1. Claims 2, 13, and 25

Claims 2, 13, and 25 require that "the at least one threshold value includes a minimum number of available routers in a backup router group." The Examiner

[30] *Ofek*, ¶ [0033].

admitted that *Ofek* and *Liu* fail to teach these limitations.[31] The Examiner cited *Yip*, col. 4, lines 30-40 as allegedly teaching these limitations. The cited portion of *Yip* teaches a ping tracking parameter obtained by pinging the IP addresses of interest, such as the IP address of a critical file server or a router's default gateway. *Yip* fails to teach or suggest that the ping tracking parameter represents a "minimum number of available routers in a backup router group" or that the parameter is included in threshold value for detecting a condition of a backup router group. For at least these additional reasons, Appellants respectfully submit that the Examiner erred in rejecting claims 2, 13, and 25.

2. Claims 7, 18, and 30

Claims 7, 18, and 30 require that "the [detected] condition is a minimum number of functional routers available in a corresponding backup router group." The Examiner admitted that *Ofek* and *Liu* fail to teach these limitations.[32] The Examiner cited *Yip* col. 4, lines 50-51 as allegedly teaching these limitations. The cited portion of *Yip* teaches a "diagnostics tracking parameter." *Yip* teaches that the tracking parameters are used to elect a master router.[33] However, *Yip* fails to teach or suggest that the diagnostics tracking parameter is used to determine whether a group includes a "minimum number of functional routers." For at least this additional reason, Appellants respectfully submit that the Examiner erred in rejecting claims 7, 18, and 30.

3. Claims 8, 19, and 31

Claims 8, 19, and 31 require that "the [detected] condition is a minimum number of functional routers available only in a corresponding backup router group." The Examiner admitted that *Ofek* and *Liu* fail to teach these limitations.[34] The Examiner cited *Yip* col. 4, lines 50-51 as allegedly teaching these limitations. The cited portion of *Yip* teaches a "diagnostics tracking parameter." *Yip* fails to

---

[31] *Office Action*, pp. 13, 15, 16 (Mar. 26, 2010).

[32] *Office Action*, pp. 13, 15, 17 (Mar. 26, 2010).

[33] *E.g.*, *Yip*, Abstract; col. 4, lines 59-61.

[34] *Office Action*, pp. 13, 15, 17 (Mar. 26, 2010).

teach or suggest that the diagnostics tracking parameter is used to detect a minimum number of functional routers in a corresponding router group, much less a minimum number of functional routers only in a corresponding router group. For at least this additional reason, Appellants respectfully submit that the Examiner erred in rejecting claims 8, 19, and 31.

C. Conclusion

For the reasons stated above, Appellants respectfully submit that the Examiner erred in rejecting all pending claims. It is believed that no extensions of time or fees are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required (including fees for net addition of claims) are hereby authorized to be charged to Hewlett-Packard Development Company's Deposit Account No. 08-2025.

Respectfully submitted,

/Jonathan M. Harris/

Jonathan M. Harris
PTO Reg. No. 44,144
CONLEY ROSE, P.C.
(713) 238-8000 (Phone)
(713) 238-8008 (Fax)
ATTORNEY FOR APPELLANTS

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
Legal Dept., M/S 35
3404 E. Harmony Road
Fort Collins, CO 80528-9599

VIII. CLAIMS APPENDIX

1. A method for monitoring a network containing routers using a backup routing protocol and organized in at least one backup router group, comprising:

discovering a topology object model of the routers;

detecting a condition of the at least one backup router group based on at least one threshold value; and

displaying an indication of the detected condition.

2. The method of Claim 1, wherein the at least one threshold value includes a minimum number of available routers in a backup router group.

3. The method of Claim 1, wherein the detecting is also based on a number of backup router groups to which one of the routers belongs.

4. The method of Claim 1, wherein for each backup router group the topology object model comprises:

at least one network router node;

at least one network interface for each at least one network router node;

at least one address for each at least one network interface;

a state of each one of the at least one address that is internal to the backup router group; and

any tracked interfaces associated with each one of the at least one address that is internal to the backup router group.

5. The method of Claim 4, wherein the topology object model comprises:

a state of at least one of the at least one address that is external to the backup router group.

6. The method of Claim 5, wherein the detecting is also based on the state of the at least one address that is external to the backup router group.

7. The method of Claim 1, wherein the condition is a minimum number of functional routers available in a corresponding backup router group.

8. The method of Claim 1, wherein the condition is a minimum number of functional routers available only in a corresponding backup router group.

9. The method of Claim 1, comprising:

receiving status information from the routers; and

updating the topology object model to reflect the received status information.

10. The method of Claim 9, wherein the status information includes states associated with interface addresses within the at least one backup router group.

11. The method of Claim 10, wherein the status information includes status of tracked interfaces associated with routers organized in the at least one backup router group.

12. A system for monitoring a network containing routers using a backup routing protocol and organized in at least one backup router group, comprising:

means for discovering a topology object model of the routers and detecting a condition of the at least one backup router group based on at least one threshold value; and

means for displaying an indication of the detected condition.

13. The system of Claim 12, wherein the at least one threshold value includes a minimum number of available routers in a backup router group.

14. The system of Claim 12, wherein the detecting is also based on a number of backup router groups to which one of the routers belongs.

15. The system of Claim 12, wherein for each backup router group the topology object model comprises:

at least one network router node;

at least one network interface for each at least one network router node;

at least one address for each at least one network interface;

a state of each one of the at least one address that is internal to the backup router group; and

any tracked interfaces associated with each one of the at least one address that is internal to the backup router group.

16. The system of Claim 15, wherein the topology object model comprises:

a state of at least one of the at least one address that is external to the backup router group.

17. The system of Claim 16, wherein the detecting is also based on the state of the at least one address that is external to the backup router group.

18. The system of Claim 12, wherein the condition is a minimum number of functional routers available in a corresponding backup router group.

19. The system of Claim 12, wherein the condition is a minimum number of functional routers available only in a corresponding backup router group.

20. The system of Claim 12, comprising:

means for receiving status information from the routers and for updating the topology object model to reflect the received status information.

21. The system of Claim 20, wherein the status information includes states associated with interface addresses within the at least one backup router group.

22. The system of Claim 21, wherein the status information includes status of tracked interfaces associated with routers organized in the at least one backup router group.

23. The system of Claim 12, wherein:

the means for discovering also receives status information from the routers and updates the topology object model to reflect the received status information.

24. A computer readable medium comprising a computer program embedded therein for causing a computer to perform:

discovering a topology object model of routers included within a network;

detecting a condition of at least one backup router group of the routers based on at least one threshold value; and

displaying an indication of the detected condition.

25. The medium of Claim 24, wherein the at least one threshold value includes a minimum number of available routers in a backup router group.

26. The medium of Claim 24, wherein the detecting is also based on a number of backup router groups to which one of the routers belongs.

27. The medium of Claim 24, wherein for each backup router group the topology object model comprises:

at least one network router node;

at least one network interface for each at least one network router node;

at least one address for each at least one network interface;

a state of each one of the at least one address that is internal to the backup router group; and

any tracked interfaces associated with each one of the at least one address that is internal to the backup router group.

28. The medium of Claim 27, wherein the topology object model comprises:

a state of at least one of the at least one address that is external to the backup router group.

29. The medium of Claim 28, wherein the detecting is also based on the state of of the at least one address that is external to the backup router group.

30. The medium of Claim 24, wherein the condition is a minimum number of functional routers available in a corresponding backup router group.

31. The medium of Claim 24, wherein the condition is a minimum number of functional routers available only in a corresponding backup router group.

32. The medium of Claim 24, wherein the computer program causes the computer to perform:

receiving status information from the routers; and

updating the topology object model to reflect the received status information.

33. The medium of Claim 32, wherein the status information includes states associated with interface addresses within the at least one backup router group.

34. The medium of claim 33, wherein the status information includes status of tracked interfaces associated with routers organized in the at least one backup router group.

35. A data structure embodied within a computer readable medium for representing a backup routing protocol topology object model for a network, the data structure comprising:

at least one network node object representing an element in the network;

at least one network interface object for each at least one network node object, the at least one network interface object representing an interface of the network element corresponding to the each at least one network node object;

an address object for each at least one network interface object, representing an address of the corresponding interface;

a backup routing protocol group object representing network elements organized in a backup routing protocol group, the backup routing protocol group object including a virtual address of the backup routing protocol group and real addresses of the network elements in the backup routing protocol group; and

an address state object for each of the real addresses of the network elements in the backup routing protocol group, including a state of the corresponding address.

36. The data structure of Claim 35, comprising:

a track interface object corresponding to a tracked network interface of a first network element in the backup routing protocol group wherein the tracked network interface is located between the first network element and a network element outside the backup routing protocol group.

37. The data structure of Claim 35, wherein:

the backup routing protocol group is related to one or more network node objects;

the backup routing protocol group is related to one or more address objects;

each network node object is related to one or more backup routing protocol group objects;

each network node object is related to one or more network interface objects;

each network interface object is related to one or more address objects; and

each address object is related to one or more network interface objects.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.